HOW TO **REDUCE** COUNTERINTELLIGENCE **RISKS**

The following practices and general guidance can help reduce your risk to targeting by potential adversaries:

Be wary of attempted contact by individuals or groups unknown to you, whether by email, phone, social media or personal encounters. Even when you know the sender of an email, ask yourself if the requested action (such as an invitation to click on a link) is consistent with your normal interactions with that person.

Be attentive to transmission of personal and work-related information, particularly via phone and web. Metadata in electronic files (including documents and photos) typically contains identifying information, including file creation timestamps and location information. Treat such information as the sensitive data it is. Where appropriate, use secure means, such as commercially available encryption, to transmit sensitive information.

Make an effort to understand and then monitor your privacy and security settings on social media sites, especially those that reveal your geographic location, and adjust them accordingly.

Be alert to any suspicious activity related to your personal electronic devices, such as spam messages from unknown senders or excessive, out-of-cycle or unusual software downloads or updates.

Talk with your immediate family members, especially those identified in your personnel records at the U.S. Office of Personnel Management, and share this same guidance. Ask them to tell you about any suspicious activities and contacts they experience.

Immediately report any suspicious activities and contacts, whether experienced by you directly or your immediate family members to DOEcounterintel@doe.gov or to your local FBI office.

When traveling overseas, you should be particularly vigilant. You should assume that your affiliation with the U.S. government is known to the foreign country you are visiting.

Don't bring sensitive materials or equipment with you, and don't discuss sensitive matters while overseas. Safeguard your personal documents.

Be alert to suspicious activities, unusual behavior, or potential compromises of your personal electronic devices; you should consider leaving them at home, taking approved equipment intended for overseas use or purchasing inexpensive, disposable equipment for your own use.

Remember that rental cars or hotel rooms, including hotel room safes, are not secure places to leave sensitive information in print or electronic format.

Make sure you understand the guidance from your local counterintelligence office on what to do if someone does approach you seeking sensitive information. And if you are approached by anybody seeking sensitive information, please report that contact to DOEcounterintel@doe.gov, your local counterintelligence office or your supervisor when you can do so safely and securely.

Avoid risky behavior or potentially or embarrassing situations when you are overseas. Foreign intelligence and security services regularly stage opportunities to create vulnerabilities, monitor and exploit weaknesses or look for misconduct overseas. This is basic tradecraft to create leverage that can be used to gain sensitive information, including through blackmail, extortion or coercion.

Know the locations and contact information for U.S. embassies or consulates for any issues or emergencies that might arise when you are overseas. **www.state.gov/travel/index**

Adversaries are willing to spend months or years developing relationships with people who have access to the information they want, including using family members. Their initial interactions may seem benign, but they may be nurturing the relationship and trying to earn your trust in small and unrelated matters. If they find nothing to encourage them or do not detect a point of leverage, they may never directly ask you to work on their behalf, but they could nevertheless use you to facilitate introduction to others you work with who may be more vulnerable.

Please report all suspicious activity to your local DOE Counterintelligence Office or local FBI field office. For obvious security reasons, we request that you avoid providing the exact details of your concerns in unclassified communications. **Additional resources are available online.**

Argonne NATIONAL LABORATORY

U.S. DEPARTMENT OF ENERGY

Argonne National Laboratory is a U.S. Department of Energy laboratory managed by UChicago Argonne, LLC.
9700 South Cass Avenue | Argonne, IL 60439 | July 2015
countrisks_fs_0715_ss

www.anl.gov